REMARKS

The Office Action mailed January 10, 2006 considered claims 1-11, 15-19, 24 and 26-29. Claims 1, 6-11, 17-19, 24 and 26-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Strentzsch et al. (US 6,256,671) hereinafter *Strentzsch*. Claims 2-5 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Strentzsch* in view of Aziz et al. (US 6,119,234) hereinafter *Aziz*. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Strentzsch* in view of Onweller (5,799,016) hereinafter *Onweller*.[1]

By this paper, claims 1, 24 and 26 have been amended such that claims 1-11, 15-19, 24, and 26-29 remain pending, of which claims 1, 24, and 26 are the only independent claims under consideration.

The invention is generally directed to facilitating domain name resolution for computer devices whose native host name data protocol is not compatible with host name data resolution protocols across a particular connection on a network. A requesting computer system may include a native host name resolver that is not capable of resolving a host name when the requesting computer system is connected to the network. The native host name resolver may be unable to resolve host names due to advances in name resolution techniques or proprietary name resolution techniques. Thus, resolving a host name may be accomplished by using a non-native replacement resolver on the computer system which is capable of resolving host names on the network. The replacement resolver receives name resolution requests from the native resolver so as to extend the functionality of the computer system. This may extend the useful life of the computer system by allowing the computer system to be used on networks that it was not originally intended to be used with.

In particular, each of the claims recites embodiments where a computer system requesting domain name resolution is assigned as its own name server. Host name data is routed *from the requesting computer system native host name resolver* using a protocol incompatible for resolution of the host name by a DNS server, *to a replacement host name resolver at the requesting computer system*. The replacement resolver can send the host name data using a

[1] Although the prior art status of the cited art is not being challenged at this time, Applicants reserve the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

second protocol that is compatible for resolving host name data over a communication link connecting the requesting computer system to the network. A resolved address is received at the native host name resolver corresponding to the host name data.

For example, claim 1 is directed to a method implemented by a computer system that requests domain name resolution. The method includes assigning the requesting computer system as a name server for the requesting computer system. The method further includes requesting resolution of a host name by sending host name data from the native host name resolver in a first protocol back to the requesting computer system as the name server assigned for the requesting computer system. The host name data is compatible for resolution of the host name by a DNS server, however, the first protocol is a native protocol of the requesting computer system that is not compatible for resolving host name data over a communications link connecting the requesting computer system to the network. The method further includes monitoring a name resolution of the requesting computer system for receiving the host name data in the first protocol from the requesting computer system. The host name data in the first protocol is rerouted to a replacement host name resolver in the requesting computer system. The host name data from the replacement host name resolver is sent using a second protocol, which is compatible for resolving host name data over a communications link connecting the requesting computer system to the network, to a module for resolving the host name data. A resolved address is received corresponding to the host name data at the native host name resolver.

Claim 24 is similar to claim 1, but includes a slightly different scope and functional 'step for' language, as opposed to some of the non-functional 'act of' language used in claim 1.

Claim 26, the last independent claim, is directed to a computer program product with computer executable instructions for performing a method similar to that of claim 1.

Applicant respectfully submits that all of the pending claims are allowable and distinguished over the art of record. In particular, the claims of the present application recite elements that are neither anticipated by nor made obvious by the art of record.

The Office Action cites *Strentzsch* as anticipating the independent claims of the present application under 35 USC 102(c). Applicants respectfully traverse this rejection, but have nonetheless amended the independent claims to more fully illustrate the novelty of the claims. *Strentzsch* showns nothing more, as it relates to the applicant's invention, than standard DNS techniques. For example, *Strentzsch* teaches that a "browser extracts the host name from the

URL in a conventional manner and sends a DNS query to a DNS server via [an] ISP." Col. 4, lines 52-44. Alternatively, a client sends a DNS query to a DNS proxy, which acts as a reduced feature DNS name server. Col. 5, lines 54-64. Alternatively still, *Strentzsch* teaches that the DNS proxy may be a fully functional DNS name server. Col. 6, lines 7-9. While *Strentzsch* points out that one DNS server can provide a referral to another DNS name server rather than an actual resolved IP address (col. 6, lines 41-44), *Strentzsch* is silent as to a native host name resolver at a requesting computer system as well as a replacement host name resolver at the same requesting computer system being used to request DNS information, as is recited by each of the independent claims of the present application. The teachings of *Strentzsch* simply show requesting DNS information from external DNS name servers. Not the rerouting of DNS requests from a native incompatible resolver *in the requesting computer system* to a compatible replacement resolver *in the requesting computer system* and then to a DNS server.

In particular, the independent claims as now amended each recite: a native host name resolver requesting resolution of a host name using *a native protocol of the requesting computer system that is* incompatible for resolving host name data over a communications link connecting the requesting computer system to the network; rerouting the host name data to a replacement host name resolver *in the requesting computer system*; and sending the host name data from the replacement resolver, using a compatible protocol, to a module (such as for example an external DNS server) for resolving the host name data. *Strentzsch* simply does not illustrate these features.

With regards to claims 2-5 and 16, the Examiner cites *Aziz* for showing a loopback. However, the teaching of *Aziz* are in direct conflict with the claims of the present application. For example, *Aziz* illustrates that an application sends a request to a stub resolver, which sends the request to a native resolver (resolver 225), which sends the request to the name server. As such, the native resolver, as a necessity, communicates using a protocol that is compatible with name resolution protocols on the network. Col. 8, lines 26-43. In direct contrast, the claims of the present application recite sending a request to a native resolver, that communicates using protocols that are incompatible for resolving host name data on the network, the native resolver sending the request to the name server assigned for the requesting computer, which is the requesting computer itself, so as to route the request to a replacement resolver that communicates

using compatible protocols. Thus, *Aziz* and the present invention teach and recite exactly opposite of one another.

The cited portions of *Aziz* are directed to resolving the situation where a native resolver cannot be modified to as to provide functionality needed *internal* to the computer system. *Aziz* is directed to carrying out secure communications, and using resolver functionality to accomplish certain aspects of the secure communication. For example, *Aziz* notes that "[t]he resolver on the authorized client is configured to use the data in the SX record to dynamically update the informaiton used by the client to handle secure communications." Col. 4, lines 13-16. *Aziz* further states that "[v]arious embodiments are implemented by customizing the resolver functionality to dynamically update a data structure on a client containing information used for secure communications with protected hosts." Col. 7, lines 28-31. *Aziz* notes that there are cases when the native resolver cannot be modified to include this functionality. Col. 8, lines 26-29. When this is true, *Aziz* teaches using a stub resolver to accomplish the functionality. Col. 8, lines 29-30. And while *Aziz* does indeed teach a loopback, the loopback is from the stub resolver to the native resolver (col. 8, lines 36-42) and not the native resolver to a replacement resolver as is recited by the claims of the present application. The native resolver in *Aziz* communicates using a native protocol that is compatible for resolving host name data over a communications link connecting the authorized computer system to the network ("When resolver 225 receives the query [from the stub resolver], it forwards it to the original NS 250....") As illustrated in Figure 2, the name server NS 250 is external to the authorized client 210. As such, the resolver 225 in *Aziz* is compatible for resolving host name data over a communications link connecting the authorized computer system to the network

In direct contrast, the claims of the present application are directed to solving problems when a native resolver does not communicate using a using *a native protocol of the requesting computer system that is* incompatible for resolving host name data over a communications link connecting the requesting computer system to the network because of the use of proprietary protocols or because of advances in DNS technology. Thus, the incompatibility is not with internal applications as is the case with *Aziz*, but rather with external network connections, which is not taught or suggested by *Aziz*.

Applicants respectfully submit therefore, that *Aziz* does not anticipate or make obvious, alone or in combination with *Strentzsch* the claims of the present application.

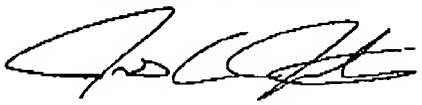
Onweller is cited by the Examiner to show UDP and TCP protocols. *Onweller* does not compensate for the deficiencies of *Hovell* and *Aziz*, however, as it relates to at least the independent claims of this application.

Furthermore, although the foregoing remarks have been focused primarily on the independent claims, it will be appreciated that all of the rejections and assertions of record with respect to the independent claims, as well as the dependent claims, are now moot, and therefore need not be addressed individually. However, in this regard, it should be appreciated that Applicant does not necessarily acquiesce to any assertions in the previous Office Action that are not specifically addressed above, and hereby reserves the right to challenge those assertions at any appropriate time in the future, should it arise, including any official notice.

In the event that the Examiner finds any remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 10 day of April, 2006.

Respectfully submitted,



RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
J. LAVAR OLDHAM
Registration No. 53,409
Attorneys for Applicant
Customer No. 47973